

SUBCHAPTER B—GENERAL REGULATIONS

PART 60—CLASSIFIED
INFORMATION

Sec.

- 60.1 Authority, scope and definitions.
- 60.2 Compliance with Executive Order 12356 and implementing directives.
- 60.3 Classification levels, categories, and limitations.
- 60.4 Limitations on original classification authority.
- 60.5 Use of derivative classification.
- 60.6 Requirements for classification guides.
- 60.7 Duration of classification.
- 60.8 Identification and markings.
- 60.9 Declassification and downgrading.
- 60.10 Access to classified information.
- 60.11 Top Secret, Secret, and Confidential Control Officer.
- 60.12 Mandatory review for declassification.
- 60.13 Custody and storage.
- 60.14 Security investigations; training and orientation of employees.
- 60.15 Debriefing upon termination of employment.
- 60.16 Responsibility of individual employees.
- 60.17 Loss or compromise; destruction of nonrecord classified information.
- 60.18 Procedures for receiving and transmitting classified documents.
- 60.19 Reproduction of classified documents.

AUTHORITY: E.O. 12356, 47 FR 14874; 32 CFR part 2001 (Directive No.1, Information Security Oversight Office), 47 FR 27836; E.O. 10450, 18 FR 2489; 22 U.S.C. 3611.

SOURCE: 53 FR 7894, Mar. 11, 1988, unless otherwise noted.

§60.1 Authority, scope, and definitions.

(a) Executive Order 12356, dated April 2, 1982 (47 FR 14874, April 6, 1982) and 32 CFR part 2001 (Directive No. 1 of the Information Security Oversight Office, approved by the National Security Council on June 22, 1982, 47 FR 27836, June 25, 1982), set forth uniform standards for the identification, classification, downgrading, declassification, and safeguarding of security information affecting the national defense and foreign relations of the United States. The regulations contained in this part are adopted pursuant to that Executive Order (which became effective on August 1, 1982) and implement its provisions within the Panama Canal Commission.

(b) Definitions:

(1) *Commission* refers to the Panama Canal Commission.

(2) *Information* means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(3) *National security information* means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(4) *Foreign government information* means:

(i) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, be held in confidence; or

(ii) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, be held in confidence.

(5) *National security* means the national defense or foreign relations of the United States.

(6) *Confidential source* means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship or both be held in confidence.

(7) *Original classification* means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

(8) *Deputy Administrator* means the U.S. citizen incumbent of that position or the U.S. citizen temporarily designated to assume the responsibilities set forth under this part. In the event

Panama Canal Regulations

§ 60.3

that the regular incumbent is not serving in the position, a senior U.S. citizen official of the Commission listed in § 60.4(a) will designate an eligible U.S. citizen to assume the duties and responsibilities of the position as set forth in this part.

(9) *Director, Office of Executive Administration*, “Deputy Director, Office of Executive Administration,” “Deputy Personnel Director,” and “Chief, Administrative Services,” are similarly defined to mean the U.S. citizen(s) temporarily designated to assume the responsibilities of the position as set forth in this part.

(10) *DUSD(P)* refers to the Deputy Under Secretary of Defense (Policy).

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.2 Compliance with Executive Order 12356 and implementing directives.

(a) The Director, Office of Executive Administration is designated the senior agency official to direct and administer the information security program for the Commission, including an active oversight and security education program to ensure effective implementation of Executive Order 12356 and any implementing directives published by the Information Security Oversight Office.

(b) The Director, Office of Executive Administration will establish procedures to prevent unnecessary access to classified information, including procedures that:

(1) Require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and

(2) Ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

(c) The Deputy Personnel Director will direct the conduct of investigations relative to the issuance of security clearances in accordance with the standards and criteria of Executive Order 10450.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.3 Classification levels, categories, and limitations.

(a) Classification levels. Official information which requires protection against unauthorized disclosure in the interest of the national security shall be classified *Top Secret*, *Secret*, or *Confidential* depending upon the degree of its significance to national security. No other terms or phrases of classification shall be used to identify such information except as otherwise expressly provided by statute. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by one of the original classification authorities listed in § 60.4(a), who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by one of the original classification authorities, who shall make this determination within thirty (30) days.

(1) *Top Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. The Commission does not have the authority to classify information originally as *Top Secret*.

(2) *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Classification categories. Information shall be considered for classification if it concerns:

(1) Military plans, weapons, or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities (including special activities), or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of Information Security, Office of the Deputy Under Secretary of Defense (Policy).

(c) Information that is determined to concern one or more of the categories in § 60.3(b) shall be classified when one of the original classification authorities listed in § 60.4(a) also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Classification on the basis of combination or association with other (classified or unclassified) information shall be supported by a written explanation which shall be maintained with the record copy of such information.

(d) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(e) Information classified in accordance with § 60.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information, see § 60.11(e).

(f) Limitations on classification.

(1) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, an organization, or the Panama Canal Commission or other agency; to restrain competition; or to prevent or delay the release of information that

does not require protection in the interest of national security.

(2) Basic scientific research information not clearly related to the national security may not be classified.

(3) The President or the officials designated by the President in the FEDERAL REGISTER may reclassify information previously declassified and disclosed if it is determined in writing that:

(i) The information requires protection in the interest of national security; and

(ii) The information may reasonably be recovered. These reclassification actions shall be reported promptly to the Office of the Deputy Under Secretary of Defense (Policy) for subsequent reporting to the Director of the Information Security Oversight Office.

(4) Information in the custody of the Panama Canal Commission may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Executive Order 12356 if such classification meets the requirements of that Executive Order and is accomplished personally and on a document-by-document basis by the officials identified in § 60.4(a) or an official with original Top Secret classification authority.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.4 Limitations on original classification authority.

(a) The authority to classify information originally under this part shall be limited to the categories of Secret and Confidential. Only the following officials of the Panama Canal Commission are authorized to classify information or material originally:

(1) The Deputy Administrator;

(2) The Director, Office of Executive Administration; and

(3) The Secretary, Washington Office.

(b) Other officials and employees of the Panama Canal Commission originating documents which, in their opinion, should be classified as Secret or Confidential prior to dispatch, shall forward these documents to the Director, Office of Executive Administration

Panama Canal Regulations

§ 60.5

with recommendation for appropriate classification. Such documents shall be protected by a cover sheet (such as Panama Canal Commission Forms 165-Conf or 165-B Secret) of the classification recommended by the originator, and shall be handled and safeguarded as if classified, see § 60.8(a).

(c) All information originated within the Commission which is believed to require classification as Top Secret (within the meaning of this part and Executive Order 12356) shall be hand carried by the originator to the Director, Office of Executive Administration who will determine the appropriate level of classification. If the information warrants Top Secret classification, that official shall transmit the information promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority in accordance with the procedures established by § 60.18 of this part. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office for a determination.

(d) Intra-office documents, such as longhand notes or draft papers, that contain information affecting the national security shall be distinctly marked with the proper classification at top and bottom, by hand, by the originator, and shall be protected and destroyed in the same manner as an inter-office or inter-agency classified documents. Such intra-office documents shall be forwarded to the Office of Executive Administration for destruction as soon as the content has been included in a formal classified paper or as soon as the note or draft is no longer required.

(e) A holder of classified information or material shall observe and respect the classification assigned by the originator.

(f) Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with Executive Order 12356 and its implementing directives. The information shall be transmitted promptly as

provided under the Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.5 Use of derivative classification.

(a) Derivative classification is: (1) the determination that information is in substance the same as information currently classified; and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions; and

(2) Carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

(c) If a person who applies derivative classification markings believes that the process of reproducing, extracting, paraphrasing, restating or summarizing may have changed the level of or removed the basis for classification, an appropriate official of the originating agency or the office of origin who has the authority to upgrade, downgrade or declassify the information must be consulted.

(d) Paper copies of derivatively classified documents shall be marked at the time of origination as follows:

(1) Classification authority. (i) The authority for classification shall be shown as follows:

CLASSIFIED BY (description of source document on classification guide).

(ii) If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown as follows:

CLASSIFIED BY MULTIPLE SOURCES

In these cases the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" shall cite the source document in its "CLASSIFIED BY" line rather than the term "MULTIPLE SOURCES."

(2) Declassification and downgrading instructions. Dates or events for automatic declassification or downgrading, or the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED" to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on a "DECLASSIFY ON" line as follows:

DECLASSIFY ON (date; description of event) or ORIGINATING AGENCY'S DETERMINATION REQUIRED (OADR)

(3) Any additional markings or abbreviations described in paragraphs (b) through (m) of § 60.8 of this part appearing on the source material shall be carried forward to the new material when appropriate.

§ 60.6 Requirements for classification guides.

(a) Classification guides used to direct derivative classification and issued pursuant to Section 2.2 of Executive Order 12356 and § 60.5 of this part shall, at a minimum:

(1) Identify or categorize the elements of information to be protected;

(2) State which of the classification designations (i.e., Top Secret, Secret, or Confidential) applies to each element or category of the information;

(3) Prescribe declassification instructions for each element or category of information in terms of:

(i) A period of time,

(ii) The occurrence of an event, or

(iii) A notation that the information shall not be declassified automatically without the approval of the originating agency; and

(4) Indicate how the designation, time limits, markings, and other requirements of Executive Order 12356 and this part are to be applied.

(b) Each classification guide shall be kept current and shall be reviewed at least once every two years and updated as necessary. The Office of Executive Administration shall compile and maintain a list of classification guides in current use.

(c) Each guide shall be approved personally and in writing by the Director, Office of Executive Administration.

(d) The Deputy Administrator may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. A decision to waive the requirement should be based, at minimum, on an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anticipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner. The Director of the Information Security Oversight Office shall be notified of any waivers.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.7 Duration of classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders

Panama Canal Regulations

§ 60.8

shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The originating agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of Executive Order 12356.

§ 60.8 Identification and markings.

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) One of the three classification levels defined in § 60.3;

(2) If the original classification authority is other than the approving or signing official, the identity shall be shown as follows:

CLASSIFIED BY (identification of original classification authority)

(3) Agency and office of origin. If the identity of the originating agency and office is not apparent on the face of a document, it shall be placed below the "CLASSIFIED BY" line.

(4) Declassification and downgrading instructions. Declassification and, as applicable, downgrading instructions shall be shown as follows:

(i) For information to be declassified automatically on a specific date:

DECLASSIFY ON: (date)

(ii) For information to be declassified automatically upon occurrence of a specific event:

DECLASSIFY ON: (description of event)

(iii) For information not to be declassified automatically:

DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED or "OADR"

(iv) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

DOWNGRADE TO (classification level) ON (date or description of event)

(b) Each classified document shall by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. The Deputy Administrator may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of Executive Order 12356, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor Executive Orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials listed in § 60.4(a) of this part.

(f) The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked or stamped at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, on the back page, and on the outside of the back cover (if any). Each interior page of a classified document shall be marked or stamped at the top and bottom either according to the highest classification of the content of the page, including the designation "Unclassified" when appropriate, or according to the highest classification of the document. In any case, the classification marking of the page shall not supersede the classification marking of

portions of the page marked with lower levels of classification.

(g) Whenever practicable, subjects and titles shall be selected so as not to require classification. When the subject or title is classified, an unclassified identifier may be assigned to facilitate receipt and reference.

(h) Classifiers shall identify the level of classification of each classified portion of a document (including subjects and titles), and those portions that are not classified. Portion marking shall be accomplished by placing a parenthetical designator immediately preceding or following the text that it governs. The symbols “(TS)” for Top Secret, “(S)” for Secret, “(C)” for Confidential, and “(U)” for Unclassified, shall be used for this purpose. If individual portion marking is impracticable, the document shall contain a description sufficient to identify the information that is classified and the level of such classification. The officials listed in §60.4(a) may for good cause, request from the DUSD(P) a waiver of the portion marking requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified by the DUSD(P) of any waivers.

(i) The classification and associated markings prescribed by this part for documents shall, where practicable, be affixed to material other than documents by stamping, tagging, or other means. If this is not practicable, recipients shall be made aware of the classification and associated markings by notification or other means.

(j) A transmittal document shall indicate on its face the highest classification of any information transmitted by it. It shall also include the following or similar instruction:

(1) For an unclassified transmittal document:

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED

(2) For a classified transmittal document:

UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (classification level of the transmittal document standing alone)

(k) Documents that contain foreign government information shall include

either the marking “FOREIGN GOVERNMENT INFORMATION,” or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin. Documents classified by a foreign government or an international organization of governments shall, if the foreign classification is not in English, be marked with the equivalent United States classification. Foreign government information not classified by a foreign government or an international organization of governments but provided to the United States in confidence by a foreign government or by an international organization of governments, shall be classified at an appropriate level and shall be marked with the United States classification accordingly.

(l) In addition to the marking requirement in paragraphs (a) through (k) of this section, the additional markings provided in paragraphs (1)(1)–(3) of this section shall, as appropriate, be displayed prominently on classified information. When display of these additional markings is not practicable, their applicability to the information shall be included in the written notification of the assigned classification.

(1) For classified information containing Restricted Data or Formerly Restricted Data as defined in the Atomic Energy Act of 1954, as amended, such markings as may be prescribed by the Department of Energy in regulations issued under the Act shall be applied.

(2) For classified information involving intelligence sources or methods:

WARNING NOTICE—INTELLIGENCE SOURCES AND METHODS INVOLVED.

(3) For classified information that, pursuant to Executive Order 12356, the originator has determined should be subject to special dissemination or reproduction limitations, or both, a statement placing the user on notice of the restrictions shall be included in the text of the document or on its cover

Panama Canal Regulations

§ 60.10

sheet; e.g., "Reproduction requires approval of originator," or "Further dissemination only as directed by the Director, Office of Executive Administration."

(m) National security information that is transmitted electronically shall be marked as follows:

(1) The highest level of classification shall appear before the first line of text;

(2) A "CLASSIFIED BY" line is not required;

(3) The duration of classification shall appear as follows:

(i) For information to be declassified automatically on a specific date:

DECL:(date)

(ii) For information to be declassified upon occurrence of a specific event:

DECL:(description of event)

(iii) For information not to be automatically declassified which requires the originating agency's determination, see § 60.7(a):

DECL: OADR

(iv) For information to be automatically downgraded:

DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur).

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.9 Declassification and downgrading.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Review of classified information shall be coordinated with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by § 60.3 of this part, despite the passage of time, will continue to be protected in accordance with Executive Order 12356 and this part.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; by the originator's successor; by a supervisory official of either; or by officials delegated such authority,

in writing, by an official listed in § 60.4(a).

(c) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of Executive Order 12356 and this part.

(d) In the case of classified information that is not officially transferred as described in § 60.9(c), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of Executive Order 12356 and this part. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(e) The Commission shall maintain a current listing of officials delegated declassification or downgrading authority by name or position.

(f) Classified information accessioned into the National Archives of the United States from the Commission shall be declassified or downgraded by the Archivist of the United States in accordance with Executive Order 12356, the directives of the Information Security Oversight Office, and guidelines established by the Director, Office of Executive Administration of the Panama Canal Commission. Such guidelines shall be reviewed and updated, if necessary, at least every five years, unless earlier review is requested by the Archivist.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§ 60.10 Access to classified information.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made and that such access is essential to the accomplishment of lawful and authorized Government purposes. The determinations of eligibility and trustworthiness, referred to in this part as a security clearance, shall be based on such investigations as the Panama Canal Commission may require. The Deputy Personnel Director

shall be responsible for conducting investigations relative to the issuance of security clearances in accordance with the standards and criteria of Executive Order 10450, and will maintain a list showing the level of security clearances granted to each person. Security clearances will be granted by the Director, Office of Executive Administration, as provided in § 60.14 of this part.

(b) In addition to a security clearance, a person must have a need for access to the particular classified information or material sought in connection with the performance of that person's official duties or contractual obligations, except in those instances provided for in paragraph (d) of this section. The determination of that need shall be made by the Director, Office of Executive Administration in coordination with officials having responsibility for the classified information or material.

(c) When a person no longer requires access to classified information or material in connection with the performance of that person's official duties or contractual obligations, the security clearance shall be withdrawn. Likewise, when a person no longer needs access to a particular security classification category, that person's security clearance shall be adjusted to the classification category still required for the performance of that person's duties and obligations. In both instances, such action shall be without prejudice to the person's eligibility for a security clearance should the need again arise.

(d) Persons engaged in historical research projects and former Presidential appointees who occupied policy-making positions may be authorized access to classified information or material originating within the Panama Canal Commission. In such cases, the requirement in section 60.10(a) that access to classified information may be granted only as is essential to the accomplishment of lawful and authorized Government purposes, may be waived, but only if the Commission has jurisdiction over the information and:

- (1) The Commission makes a written determination that access is consistent with the interests of national security;
- (2) The Commission takes appropriate steps to protect classified information

from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with Executive Order 12356;

(3) The Commission limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee; and

(4) In addition, the Director, Office of Executive Administration obtains:

(i) Written agreements from the requesters to safeguard the information to which they are given access, as permitted by Executive Order 12356 and this part; and

(ii) Written consent from the requester for the Director, Office of Executive Administration to review all of their notes and manuscripts for the purpose of assuring that no classified information is contained in them.

(e) If the access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to 31 U.S.C. 9701, the requesters shall be so notified and the fees may be imposed.

(f) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59883, Nov. 26, 1991]

§ 60.11 Top Secret, Secret, and Confidential Control Officer.

(a) The Director, Office of Executive Administration, Panama Canal Commission, is the Agency's designated Top Secret Control Officer and is responsible for the receipt, current accountability, and transmission of all Top Secret information. The Deputy Director, Office of Executive Administration is the Alternate Top Secret Control Officer. A physical inventory of all Top Secret material shall be made at least annually.

(b) The Director and the Deputy Director, Office of Executive Administration are also the Agency's designated Control Officer and Alternate Control

Panama Canal Regulations

§ 60.12

Officer, respectively, for all classified information up to and including Secret.

(c) The Director, Office of Executive Administration shall act on all suggestions and complaints received by the Commission with respect to the administration of Executive Order 12356 and this part, and may also recommend to the Deputy Administrator appropriate administrative actions or sanctions to correct abuse or violation of any provision of that Order or directives under it. The Director of the Information Security Oversight Office shall be promptly informed by the agency when such violations occur.

(d) To the extent required by applicable laws and agency regulations, the Deputy Administrator shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

(e) When the Commission is the agency of primary interest, following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with the Executive Order 12356 or predecessor orders, the Director, Office of Executive Administration shall determine the degree of damage to the national security, the need for continued classification, and, in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences, see § 60.17.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59883, Nov. 26, 1991]

§ 60.12 Mandatory review for declassification.

(a) Any United States citizen, permanent resident alien, federal agency, or the government of a U.S. state or municipality may request that classified information be reviewed for declassification by the originating agency and released. Such requests must be submitted in writing to the Chief, Administrative Services Division, Panama Canal Commission, Unit 2300, APO AA 34011-2300 (or Panama Canal Com-

mission, Balboa Heights, Republic of Panama). In accordance with section 9701 of title 31, United States Code, fees may be applied to any requests for declassification and release. A request need not identify the information requested by date or title, but must describe the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort. Whenever a request is deficient in its description of the information sought, the Chief, Administrative Services Division shall notify the requester that, unless additional identifying information is provided or the scope of the request is narrowed, the Commission will take no further action on the request.

(b) When the Commission receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response is required, it is the responsibility of the referring agency to respond to the requester.

(c) When another agency refers a request to the Commission for review because the Commission originally classified the information requested, the Commission shall treat the request as though it were submitted directly to it under paragraph (a) of this section. The Commission shall send its decision directly to the requester and shall, if so requested, notify the referring agency of its decision on the request and on the appeal, if any.

(d) Requests for classification review made under paragraph (a) of this section shall be promptly acknowledged by the Chief, Administrative Services Division and then forwarded to the official who originally classified the document, or that official's successor, or when appropriate to an official designated by an official listed in § 60.4(a), who, in coordination with the Chief, Administrative Services Division, shall

decide whether the requested information may be declassified, see § 60.7 and § 60.9.

(1) Unless withholding is otherwise warranted under applicable law, any information which may be declassified shall normally be forwarded to the requester within sixty (60) days after receipt of a proper request. If additional time is needed to locate or review the requested information, the Chief, Administrative Services Division will notify the requester accordingly. Except in unusual circumstances, a decision will be made within one year of receipt of the request.

(2) When information cannot be declassified in its entirety, a reasonable effort will be made, consistent with other applicable law, to release those portions of the requested information that constitute a coherent segment.

(3) Upon the denial or a partial denial of a request, the Chief, Administrative Services Division shall reply to the requester and provide a brief statement of the reasons for the denial, a notice of the right to appeal the decision to the Director, Office of Executive Administration and a notice that the appeal must be in writing and must be received by the Commission within sixty (60) days of receipt of the decision letter by the requester. Appeals should be addressed to: Director, Office of Executive Administration, Panama Canal Commission, Unit 2300, APO AA 34011-2300 (or Panama Canal Commission, Balboa Heights, Republic of Panama).

(e) Within thirty (30) days after its receipt of a proper appeal against an initial decision not to declassify information, the Director, Office of Executive Administration shall make and dispatch the decision whether the information should be declassified. If the Director, Office of Executive Administration is the original classification authority of the information under appeal, the Deputy Administrator shall determine whether the information may be declassified. The Director, Office of Executive Administration shall, after the decision, promptly make available to the requester any information that is declassified and which is otherwise releasable. If continued classification of the requested information is necessary, the requester shall be no-

tified of that decision and the reasons therefor. If requested, the appeal determination shall also be communicated to any referring agency.

(f) The classification reviews made in response to requests and appeals under this section are in addition to the systematic review of classified information prescribed by Executive Order 12356 and 32 CFR part 2001.

(g) Requests for access to classified material submitted under the Freedom of Information Act or the Privacy Act of 1974 (5 U.S.C. 552 and 552a) shall be processed in accordance with parts 9 and 10 of 35 CFR, and shall be subject to the same review criteria for declassification as requests submitted under paragraphs (a) through (d) of this section. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order, the Commission shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under Executive Order 12356 or 32 CFR part 2001.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59883, Nov. 26, 1991; 59 FR 26123, May 19, 1994]

§ 60.13 Custody and storage.

(a) Classified information shall be protected in accordance with applicable National Security Council directives or directives promulgated by the Information Security Oversight Office and approved by the National Security Council.

(b) Each bureau director and chief of an independent unit (or classified security control officer as designated by the Director, Office of Executive Administration) shall be responsible for assuring that all classified information within that official's organization is used, processed, stored, and transmitted only under conditions which will provide adequate protection and prevent access by, or dissemination to, unauthorized persons. Containers, vaults, alarm systems, and associated security devices procured after the effective date of this part for the storage and protection of classified information

Panama Canal Regulations

§ 60.13

shall be in conformance with the standards and specifications published by the General Services Administration and, to the maximum extent practicable, be of the type designated on its Federal Supply Schedule.

(c)(1) Top secret information shall be stored in a GSA-approved security container with an approved built-in, three-position, dial-type combination lock; in a vault protected by an alarm system and response force; or in other storage facility that meets the standards for top secret established under the provisions of paragraph (b) of this section.

(2) Secret and confidential information shall be stored in a manner and under the conditions prescribed for top secret information, or in a container, vault, or alarmed area that meets the standards for secret or confidential information established pursuant to the provisions of paragraph (c)(1) of this section, and/or paragraph (c)(3) of this section.

(3) Secret and confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type, changeable combination lock, or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a three-position, changeable combination padlock approved by GSA for the purpose. The Director, Office of Executive Administration shall prescribe any necessary supplementary controls for storage of secret information in cabinets equipped with a steel lock bar.

(d) Each bureau director and chief of an independent unit (or classified security control officer) is responsible for assuring that all personnel within that official's organization, having access to classified information, have a security clearance issued by the Director, Office of Executive Administration, see § 60.14 and § 60.16.

(e)(1) Combinations of all repositories containing classified information shall be changed at least annually and forwarded in double-sealed envelopes to the Office of Executive Administration. The double-sealed envelopes shall be classified no lower than the highest category of information contained in the repositories. Combinations to dial-type locks shall be changed only by

persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to the combination, whenever the equipment is taken out of service, and at least once every year. Knowledge of combinations protecting classified information shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information to be stored in the security equipment concerned. Bureau directors and heads of independent units (or classified security control officers) shall ensure that combinations of dial-type locks shall be changed whenever there is reason to suspect possible compromise of the current combination.

(2) When security equipment having a built-in combination lock is taken out of service, the lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(3) The Commission shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected. Under no circumstances may keys be removed from the premises. They shall be stored in a secure container.

(f) Custodians of classified matter are responsible for registering with the Office of Executive Administration the names of all persons having knowledge of combinations to repositories containing classified information.

(1) Persons entrusted with classified information shall be responsible for providing protection and accountability for such information at all times and for locking classified information in approved security equipment whenever it is not in use or under the direct supervision of authorized persons. Custodians shall follow procedures which will ensure that unauthorized persons do not gain access to classified information.

(2) Individuals charged with the custody of classified information shall

§ 60.14

conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. The Director, Office of Executive Administration shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by agency regulations are in effect at all times.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59883, Nov. 26, 1991]

§ 60.14 Security investigations; training and orientation of employees.

(a) Requests for security clearances, including changes in the level of clearances, will be forwarded to the Office of Personnel Administration for background investigations and security checks. The Deputy Personnel Director shall ensure that all necessary investigations are completed, and will provide a recommendation on the issuance of a security clearance to the Office of Executive Administration. The Director, Office of Executive Administration, in consideration of all available information, will determine if a security clearance may be issued, or if the level may be changed, and establish the expiration date of the clearance.

(b) The Director, Office of Executive Administration is also responsible for establishing and maintaining a training and orientation program for employees concerned with classified information or material.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59884, Nov. 26, 1991]

§ 60.15 Debriefing upon termination of employment.

(a) Bureau directors and heads of independent units (or classified security control officers as designated by the Director, Office of Executive Administration) shall be responsible for notifying the Office of Executive Administration whenever it is necessary that an employee be briefed or debriefed. Such notification should be in writing and be at least sixty (60) days, or as long as possible, in advance.

(b) Bureau directors and heads of independent units (or classified security control officers) shall ensure that debriefings are accomplished for any employee whose employment is termi-

35 CFR Ch. I (7–1–97 Edition)

nated, or scheduled to be terminated, or when a temporary separation from employment (not to include leave) for sixty (60) days or more has occurred or is scheduled, whenever the employee has had access to classified information within the last twelve calendar months of his employment.

[56 FR 59884, Nov. 26, 1991]

§ 60.16 Responsibility of individual employees.

(a) The responsibility for the safeguarding of classified information shall rest on each individual employee having possession or knowledge of it, regardless of how such information or knowledge was obtained. In addition, each individual employee is directly responsible for acquiring familiarity with and complying with these and subsequently published security regulations.

(b) Any officer or employee, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by Executive Order 12356 or under this part, is subject to prompt and stringent administrative action, and, where a violation of criminal statute may be involved, is subject to prosecution under applicable law.

§ 60.17 Loss or compromise; destruction of nonrecord classified information.

(a) Any person who has knowledge of the loss or possible compromise of classified information in the custody of the Commission shall immediately report the circumstances to the Office of Executive Administration. The Director, Office of Executive Administration shall initiate an inquiry to:

- (1) determine cause,
- (2) place responsibility, and

(3) take corrective measures and appropriate administrative, disciplinary, or legal action. If it is determined that classified information has been compromised, the agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise.

(b) The Deputy Administrator or the Director, Office of Executive Administration shall initiate a damage assessment whenever there has been a compromise of classified information originated by the Commission that, in his judgment, can reasonably be expected to cause damage to the national security. Damage assessments shall be in writing and shall conform to the guidelines established by the Information Security Oversight Office, as provided in 32 CFR 2001.47(b).

(c) Nonrecord classified information that has served its intended purpose shall be destroyed in accordance with procedures and methods approved by the Deputy Administrator or the Director, Office of Executive Administration. The method of destruction selected must preclude recognition or reconstruction of the classified information or material.

(d) The Office of Executive Administration is the only office within the Commission authorized to destroy classified documents which have been recorded as received and assigned a control number.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59884, Nov. 26, 1991]

§ 60.18 Procedures for receiving and transmitting classified documents.

(a) The procedures for handling classified documents received by any person or unit of the Panama Canal Commission shall be as follows:

(1) All classified documents received by any person or unit of the Commission shall be immediately delivered to the Office of Executive Administration. Personnel of the Office of Executive Administration shall receipt for and record all classified documents received from outside agencies (except that those officials listed in § 60.4(a) of this part may receipt for classified documents from outside agencies, and then forward them to the Office of Executive Administration, in person or by an authorized representative).

(2) The receipted documents shall be permanently recorded by the Office of Executive Administration, at which time accountability for these documents shall be assumed by that office.

(3) When classified documents addressed to an individual in the Panama

Canal Commission are received by the Office of Executive Administration, the addressee shall be notified by telephone that such classified matter is awaiting him; or the classified documents may be transmitted as provided in paragraph (c) and (d) of this section. When the addressee picks up the classified documents, all items shall be recorded on an individual classified documents register furnished by the Office of Executive Administration; one copy is to be permanently retained in the library, and one is to be furnished to the addressee, or his authorized representative, who shall sign for the documents opposite each item on the register. This method of transfer may be utilized in lieu of a receipt.

(b) When any unit of the Panama Canal Commission prepares a document which is to be classified Secret or Confidential for transmission to other offices of the Commission, the procedure shall be as follows:

(1) Prepare sufficient copies of the document for whatever distribution is required, and one additional copy for file in the Office of Executive Administration.

(2) Forward draft copies, handwritten copies, and carbons to the Office of Executive Administration for retention or destruction under established procedures.

(i) In addition, all portions of electric typewriter ribbons used in the preparation of classified material must be destroyed in the same manner. Reusable cloth typewriter ribbons must be protected if used for preparation of classified material on the first pass through typewriter.

(ii) Classified material may not be entered into electronic equipment with memory capability, such as word processors, computers, personal computers, memory typewriters and other similar equipment, *unless* specific, written permission is obtained in advance, for each specific piece of equipment or system, from the Office of Executive Administration.

(3) Bring all copies of the document to the Office of Executive Administration. Copies shall be securely fastened underneath a cover sheet of the classification recommended by the originator.

(4) At the direction of the Director, Office of Executive Administration, the proper classification, short title, and serial number shall be assigned to each document, and an accountability stamp shall be placed on each copy.

(5) All classified documents shall be appropriately and conspicuously marked to put all persons on clear notice of their classified content. In addition, all classified documents shall be marked to indicate the downgrading-declassification schedule to be followed in accordance with § 60.9.

(6) The documents shall be recorded in the permanent documents log. The accountability for the documents passes from the originator to the Office of Executive Administration at this point.

(7) Distribution of the remaining copies shall be made according to the procedures covered in paragraphs (a)(3), (c) and (d) of this section. The number of copies of documents containing classified information shall be kept to a minimum to decrease the risk of compromise and reduce storage costs.

(c) When any unit of the Panama Canal Commission transmits documents or information classified Top Secret to other offices of the Commission, or any classified documents or information to any agencies or units other than the Commission, the procedure for handling such information shall be as follows:

(1) The documents or information shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents.

(2) A receipt shall be attached to or enclosed in the inner cover. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender.

(d) When the Commission transmits classified documents or information to any agency other than the Commission, or documents or information classified Top Secret to other offices of the

Commission, one or more of the following methods shall be used:

(1) By specifically designated personnel having the appropriate security clearance;

(2) By State Department diplomatic pouch;

(3) By messenger-courier system specifically created for that purpose;

(4) Over authorized secure communication circuits.

(e) Secret and confidential documents or information may also be transmitted by the following methods:

(1) As provided in paragraph (c) of this section, if transmittal is to be within the Commission;

(2) By U.S. registered mail through Army, Navy, or Air Force Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system; or

(3) Under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government-contract vehicles or aircraft, ships of the United States Navy, civil-service-manned U.S. Naval ships, and ships of U.S. Registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

§ 60.19 Reproduction of classified documents.

(a) Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office. The reproduction of Secret and Confidential documents may be restricted by the originating agency. Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

(b) The Office of Executive Administration is the only office within the Panama Canal Commission authorized to reproduce documents which have been classified. Other offices within the Panama Canal Commission which require the reproduction of classified documents shall take them to the Office of Executive Administration,

Panama Canal Regulations

Pt. 61

where the documents will be reproduced, properly marked, controlled and then returned to the user.

PART 61—HEALTH, SANITATION, AND COMMUNICABLE DISEASE SURVEILLANCE

Subparts A–D [Reserved]

Subpart E—Maritime Communicable Disease Surveillance

DEFINITIONS AND GENERAL PROVISIONS

Sec.

- 61.121 Purpose.
- 61.122 Definitions.
- 61.123 Periods of isolation and surveillance.
- 61.124 Periods of immunity.
- 61.125 Sanitary measures previously applied.
- 61.126 Certificate of measures applied.

MEASURES IN TRANSIT

- 61.151 Vessels; general provisions.
- 61.152 Vessels; sanitary inspection and corrective measures.
- 61.153 Vessels; entries in the official record.
- 61.154 Vessels; radio report of disease aboard.
- 61.155 Vessels; yellow fever.
- 61.156 Vessels; disinsecting.

VESSELS SUBJECT TO COMMUNICABLE DISEASE SURVEILLANCE INSPECTION

- 61.171 General provisions.
- 61.172 Exempt vessels subject to sanitary regulations.
- 61.173 Report of disease or rodent mortality on vessel during stay in port.

GENERAL REQUIREMENTS UPON ARRIVAL AT THE PANAMA CANAL

- 61.191 Applicability.
- 61.192 Vessels; awaiting inspection.
- 61.193 Maritime communicable disease surveillance declaration.
- 61.194 Persons; restrictions on boarding and leaving vessels, or having contact with persons aboard.
- 61.195 Communicable disease surveillance inspection and controls.
- 61.196 Persons; examination.
- 61.197 Vessels; persons and things; communicable diseases other than quarantinable diseases.
- 61.198 Persons; isolation.
- 61.199 Furnishing of fresh crew.
- 61.200 Disinfection of cargo.
- 61.201 Exemption for mails.

PARTICULAR REQUIREMENTS UPON ARRIVAL AT THE PANAMA CANAL

- 61.221 Applicability.

- 61.222 Cholera; vessels and things.
- 61.223 Cholera; vessels; persons.
- 61.224 Plague; vessels.
- 61.225 Plague; vessels; persons; things.
- 61.226 Yellow fever; vessels; classification.
- 61.227 Yellow fever; vessels; persons.

SANITARY INSPECTION: RODENT AND VERMIN CONTROL

- 61.241 General provisions.
- 61.242 Disinsecting and disinfection; vessels and persons.
- 61.243 Deratting Certificates; Deratting Exemption Certificates.
- 61.244 Vessels in traffic between the United States and Panama.

PRATIQUE: VESSELS

- 61.261 General requirements.
- 61.262 Free pratique.
- 61.263 Provisional pratique.
- 61.264 Radio pratique.

IMPORTATION OF DOGS AND CATS

- 61.281 Quarantine of dogs and cats.

Subpart F—Pest Exterminators

- 61.311 License required to engage in business of pest extermination.
- 61.312 Licensed foreman required to be in charge.
- 61.313 Possession and display of licenses.
- 61.314 Renewal of licenses; suspension and revocation.
- 61.315 Approval of types, concentrations, and manner of use of insecticides and rodenticides required.
- 61.316 Sale of insecticides and rodenticides.
- 61.317 Inapplicability to Government agencies and their officers and employees.
- 61.318 Inapplicability to military reservations.

Subparts G–H—[Reserved]

Subpart I—Authority of Governor

- 61.381 Authority of Governor.

AUTHORITY: Issued under authority vested in the President by section 1701, Pub. L. 96-70, 93 Stat. 492; EO 12173, 44 FR 69271.

SOURCE: 31 FR 12236, Sept. 16, 1966, unless otherwise noted.

Subparts A–D [Reserved]

Subpart E—Maritime Communicable Disease Surveillance

AUTHORITY: Issued under authority vested in the President by 22 U.S.C. 3811; EO 12215, 45 FR 36043.